APPENDIX A

Each table provides the function name and a brief usage description.

Function Name	Function Usage
pkail_cert_check	Verify a certificate as having valid "not before" and "not after" dates, and that other certificate fields are correct.
pkail_cert_create	Create a certificate entry. calls pkail_cert_decompose, pkail_cert_sig_check, pkail_cert_check
pkail_cert_decompose	Decompose a certificate into it's individual fields and move these field values into pkail_cert_fields structure
pkail_cert_sig_check	Verify a certificate as having valid digital signature. Calls pkail_rsaverify
pkail_disk_getcert	Request pkail_oper daemon to retrieve a ASN.1 BER formatted cert from pkail disk located database
pkail_disk_putcert	Request pkail_oper daemon to store a ASN.1 BER formatted cert in pkail disk located database
pkail_fndcert	Locate and return ASN.1 BER formatted cert to requester. Calls pkail_disk_getcert
pkail_loadcert	Process new certificate received from user space for loading into pkail kernel storage and pkail disk database. Calls pkail_cert_create, pkail_disk_putcert

Table 1 PKAI Certificate Specific kernel Functions

Function Name	Function Usage
pkail_keyedmd5sign	Generate a prefix-postfix keyed MD5 digital signature. Calls pkail_skey_get, pkail_md5
pkail_keyedmd5ver	Verify a prefix-postfix keyed MD5 digital signature Calls pkail_skey_get, pkail_md5
pkail_md5	Generate secret Prefix Postfix keyed MD5 message hash operation resulting in a secret key digital signature
pkail_setspi	Process a secret key entry for secret keys used with the keyed MD5 authentication. Calls pkail_skey_get, pkail_skey_create
pkail_skey_create	Create a secret key entry for secret keysin pkail_skey_list
pkail_skey_get	Locate a secret key entry by searching the pkail_skey_list for a match on pkail_skey_list.addr and pkail_skey_list.spi and when found return pkail_skey_list.key of pkail_skey_list.klen

Table 2 PKAI Secret Key Specific kernel Functions

APPENDIX A

Function Name	Function Usage
pkail_rsasign	Process request to generate an RSA digital signature. Calls pkail_privkey_get, pkail_rsa512sign, pkail_rsa768sign, pkail_rsa1024sign, pkail_rsa2048sign
pkail_rsa512sign	Generate an RSA 512 bit digital signature
pkail_rsa768sign	Generate an RSA 768 bit digital signature
pkail_rsa1024sign	Generate an RSA 1024 bit digital signature
pkail_rsa2048sign	Generate an RSA 2048 bit digital signature
pkail_rsaverify	Verify an RSA digital signature. Calls pkail_pubkey_get, pkail_rsa512ver, pkail_rsa768ver, pkail_rsa1024ver, pkail_rsa2048ver
pkail_rsa512ver	Verify an RSA 512 bit digital signature
pkail_rsa768ver	Verify an RSA 7688 bit digital signature
pkail_rsa1024ver	Verify an RSA 1024 bit digital signature
pkail_rsa2048ver	Verify an RSA 2048 bit digital signature
pkail_rsaencryp	Encrypt up to 4096 bytes of requester text. Calls pkail_privkey_get, pkail_rsa512encryp, pkail_rsa768encryp, pkail_rsa1024encryp, pkail_rsa2048encryp
pkail_rsa512encryp	Encrypt up to 4096 bytes of requester text using an RSA 512 bit public key
pkail_rsa768encryp	Encrypt up to 4096 bytes of requester text using an RSA 768 bit public key
pkail_rsa1024encryp	Encrypt up to 4096 bytes of requester text using an RSA 1024 bit public key
pkail_rsa2048encryp	Encrypt up to 4096 bytes of requester text using an RSA 2048 bit public key
pkail_rsadecryp	Decrypt up to 4096 bytes of requester text. Calls pkail_pubkey_get, pkail_rsa512decryp, pkail_rsa768decryp, pkail_rsa1024decryp, pkail_rsa2048decryp
pkail_rsa512decryp	Decrypt up to 4096 bytes of requester text using an RSA 512 bit private key
pkail_rsa768decryp	Decrypt up to 4096 bytes of requester text using an RSA 768 bit private key
pkail_rsa1024decryp	Decrypt up to 4096 bytes of requester text using an RSA 1024 bit private key
pkail_rsa2048decryp	Decrypt up to 4096 bytes of requester text using an RSA 2048 bit private key

Table 3 PKAI RSA Specific kernel Functions

APPENDIX A

Function Name	Function Usage
pkail_ecsign	Process request to generate an EC digital signature. Calls pkail_privkey_get, pkail_ec80sign, pkail_ec120sign, pkail_ec1160sign
pkail_ec80sign	Generate an EC 80 bit digital signature
pkail_ec120sign	Generate an EC 120 bit digital signature
pkail_ec160sign	Generate an EC 160 bit digital signature
pkail_ecverify	Verify an EC digital signature. Calls pkail_pubkey_get, pkail_ec80ver, pkail_ec120ver, pkail_ec160ver
pkail_ec80ver	Verify an EC 80 bit digital signature
pkail_ec120ver	Verify an EC 120 bit digital signature
pkail_ec160ver	Verify an EC 160 bit digital signature
pkail_ecencryp	Encrypt up to 4096 bytes of requester text. Calls pkail_privkey_get, pkail_ec80encryp, pkail_ec120encryp, pkail_ec160encryp
pkail_ec80encryp	Encrypt up to 4096 bytes of requester text using an EC 80 bit public key
pkail_ec120encryp	Encrypt up to 4096 bytes of requester text using an EC 120 bit public key
pkail_ec160encryp	Encrypt up to 4096 bytes of requester text using an EC 160 bit public key
pkail_ecdecryp	Decrypt up to 4096 bytes of requester text. Calls pkail_pubkey_get, pkail_ec80decryp, pkail_ec120decryp, pkail_ec160decryp
pkail_ec80decryp	Decrypt up to 4096 bytes of requester text using an EC 80 bit private key
pkail_ec120decryp	Decrypt up to 4096 bytes of requester text using an EC 120 bit private key
pkail_ec160decryp	Decrypt up to 4096 bytes of requester text using an EC 160 bit private key

Table 4 PKAI EC Specific kernel Functions

Function Name	Function Usage
pkail_dsssign	Generate a DSS 512 bit digital signature
pkail_dssverify	Verify a DSS 512 bit digital signature

Table 5 PKAI DSS Specific kernel Functions

APPENDIX A

Function Name	Function Usage
pkail_cleartables	Clear out all pkail kernel tables by overwriting with zeros, de-allocating memory, close sockets from pkail kernel services to pkail daemons
pkail_core	Identify requested pkail kernel service and call required action functions
pkail_err	General pkail kernel services function for logging errors to sys log
pkail_opensockets	Open sockets from pkail kernel services to pkail daemons
pkail_pphrase	process part of passphrase received from user space
pkail_privkey_create	create a private key entry. Calls pkail_privkey_get
pkail_privkey_get	Locate a private key, search the pkail_privkey_list for a match on either pkail_privkey_list.my_ip_addr or pkail_privkey_list.my_host_name
pkail_pubkey_get	Locate a public key, search the pkail_cert_list for a match on either pkail_cert_list.subj_ip_addr or pkail_cert_list.subj_host_name and when found return pkail_cert_list.pubkey
sys_soc_pkail	Receive UDP socket service calls from user space clients of pkail kernel services.
sys_pkail	Receive system service calls from user space clients of pkail kernel services. Calls verify_area and pkail_core

Table 6 PKAI Common kernel Functions